EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S6	42	"5781534"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/03/30 08:29
S7	56	"6334190"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/03/30 09:08
S8	155	addition same csa same multipl$5 same (cla or carry adder)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/03/30 09:45
S9	32	addition same csa same (multiplexer mux) same (cla or carry adder)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/03/30 09:57
S10	1	addition same csa same (multiplexer mux) same (cla or carry adder) and sha-1	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/03/30 09:58
S11	2	csa same (multiplexer mux) same (cla or carry adder) and sha-1	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/03/30 10:20
S12	7	csa same (multiplexer mux) same (cla or carry adder) and (sha-1 authentication)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/03/30 14:35
S13	2281978	tim$3 with critical path	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/03/30 14:35

EAST Search History

S14	4108	tim$3 with critical with path	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/03/30 14:35
S15	4	tim$3 with critical with path with hash	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/03/30 14:36
S16	7	tim$3 with critical with path same hash	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/03/30 14:36

PORTAL
USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

sha-1 and cla and csa

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used **sha 1** Found **191** of **173,942**

Sort results by: relevance
Display results: expanded form

Save results to a Binder
Search Tips
□ Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 191 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Relevance scale

1 Exploration for advanced SoC design: An HMAC processor with integrated SHA-1 and MD5 algorithms

Mao-Yin Wang, Chih-Pin Su, Chih-Tsun Huang, Cheng-Wen Wu

January 2004 **Proceedings of the 2004 conference on Asia South Pacific design automation: electronic design and solution fair ASP-DAC '04 , Proceedings of the 2004 conference on Asia South Pacific design automation: electronic design and solution fair ASP-DAC '04**

Publisher: IEEE Press , IEEE Press

Full text available: pdf(60.57 KB) Publisher Site
Additional Information: full citation, abstract, references

Cryptographic algorithms are prevalent and important in digital communications and storage, e.g., both SHA-1 and MD5 algorithms are widely used hash functions in IPSec and SSL for checking the data integrity. In this paper, we propose a hardware architecture for the standard HMAC function that supports both. Our HMAC design automatically generates the padding words and reuses the key for consecutive HMAC jobs that use the same key. We have also implemented the HMAC design in silicon. Compared wi ...

2 Secure Data Publishing and Certificate Management: Tangler: a censorship-resistant publishing system based on document entanglements

Marc Waldman, David Mazières

November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security**

Publisher: ACM Press

Full text available: pdf(149.02 KB)
Additional Information: full citation, abstract, references, citings, index terms

We describe the design of a censorship-resistant system that employs a unique document storage mechanism. Newly published documents are dependent on the blocks of previously published documents. We call this dependency an *entanglement*. Entanglement makes replication of previously published content an intrinsic part of the publication process. Groups of files, called collections, can be published together and named in a host-independent manner. Individual documents within a collection can ...

3 Embedded applications: Encryption overhead in embedded systems and sensor network nodes: modeling and analysis

Ramnath Venugopalan, Prasanth Ganesan, Pushkin Peddabachagari, Alexander Dean, Frank

Mueller, Mihail Sichitiu
October 2003 **Proceedings of the 2003 international conference on Compilers, architecture and synthesis for embedded systems**
Publisher: ACM Press
Full text available: pdf(293.59 KB) Additional Information: full citation, abstract, references, citings, index terms

Recent research in sensor networks has raised issues of security for small embedded devices. Security concerns are motivated by the deployment of a large number of sensory devices in the field. Limitations in processing power, battery life, communication bandwidth and memory constrain the applicability of existing cryptography standards for small embedded devices. A mismatch between wide arithmetic for security (32 bit word operations) and embedded data bus widths (often only 8 or 16 bits) combi ...

Keywords: embedded systems, encryption, security, sensor networks

4 Performance Considerations for an Embedded Implementation of OMA DRM 2
Daniel Thull, Roberto Sannino
March 2005 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 3 DATE '05**
Publisher: IEEE Computer Society
Full text available: pdf(139.35 KB) Additional Information: full citation, abstract, citings

As digital content services gain importance in the mobile world, Digital Rights Management (DRM) applications will become a key component of mobile terminals. This paper examines the effect dedicated hardware macros for specific cryptographic functions have on the performance of a mobile terminal that supports version 2 of the open standard for Digital Rights Management defined by the Open Mobile Alliance (OMA). Following a general description of the standard, the paper contains a detailed analy ...

Keywords: DRM, Security, Mobile Terminal, Cryptography

5 Low traffic overlay networks with large routing tables
Chunqiang Tang, Melissa J. Buco, Rong N. Chang, Sandhya Dwarkadas, Laura Z. Luan, Edward So, Christopher Ward
June 2005 **ACM SIGMETRICS Performance Evaluation Review , Proceedings of the 2005 ACM SIGMETRICS international conference on Measurement and modeling of computer systems SIGMETRICS '05**, Volume 33 Issue 1
Publisher: ACM Press
Full text available: pdf(269.80 KB) Additional Information: full citation, abstract, references, index terms

The routing tables of Distributed Hash Tables (DHTs) can vary from size $O(1)$ to $O(n)$. Currently, what is lacking is an analytic framework to suggest the optimal routing table size for a given workload. This paper (1) compares DHTs with $O(1)$ to $O(n)$ routing tables and identifies some good design points; and (2) proposes protocols to realize the potential of those good design points.We use total traffic as the uniform metric to compare heterogeneous DHTs a ...

Keywords: distributed hash table, overlay network, peer-to-peer system

6 Security: Analyzing and modeling encryption overhead for sensor network nodes
Prasanth Ganesan, Ramnath Venugopalan, Pushkin Peddabachagari, Alexander Dean, Frank Mueller, Mihail Sichitiu
September 2003 **Proceedings of the 2nd ACM international conference on Wireless**

sensor networks and applications
Publisher: ACM Press
Full text available: pdf(254.57 KB) Additional Information: full citation, abstract, references, index terms

Recent research in sensor networks has raised security issues for small embedded devices. Security concerns are motivated by the deployment of a large number of sensory devices in the field. Limitations in processing power, battery life, communication bandwidth and memory constrain the applicability of existing cryptography standards for small embedded devices. A mismatch between wide arithmetic for security (32 bit word operations) and embedded data bus widths (often only 8 or 16 bits) combined ...

Keywords: analysis, embedded systems, encryption overhead, model, sensor networks

7 Pioneer: verifying code integrity and enforcing untampered code execution on legacy systems
Arvind Seshadri, Mark Luk, Elaine Shi, Adrian Perrig, Leendert van Doorn, Pradeep Khosla
October 2005 **ACM SIGOPS Operating Systems Review , Proceedings of the twentieth ACM symposium on Operating systems principles SOSP '05**, Volume 39 Issue 5
Publisher: ACM Press
Full text available: pdf(264.30 KB) Additional Information: full citation, abstract, references, index terms

We propose a primitive, called Pioneer, as a first step towards verifiable code execution on untrusted legacy hosts. Pioneer does not require any hardware support such as secure co-processors or CPU-architecture extensions. We implement Pioneer on an Intel Pentium IV Xeon processor. Pioneer can be used as a basic building block to build security systems. We demonstrate this by building a kernel rootkit detector.

Keywords: dynamic root of trust, rootkit detection, self-check-summing code, software-based code attestation, verifiable code execution

8 Fast and secure distributed read-only file system
Kevin Fu, M. Frans Kaashoek, David Mazières
February 2002 **ACM Transactions on Computer Systems (TOCS)**, Volume 20 Issue 1
Publisher: ACM Press
Full text available: pdf(317.54 KB) Additional Information: full citation, abstract, references, index terms

Internet users increasingly rely on publicly available data for everything from software installation to investment decisions. Unfortunately, the vast majority of public content on the Internet comes with no integrity or authenticity guarantees. This paper presents the self-certifying read-only file system, a content distribution system providing secure, scalable access to public, read-only data.The read-only file system makes the security of published content independent from that of the distri ...

Keywords: File systems, read-only, security

9 A public-key based secure mobile IP
John Zao, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, Isidro Castineyra, Stephen Kent
October 1999 **Wireless Networks**, Volume 5 Issue 5
Publisher: Kluwer Academic Publishers
Full text available: pdf(255.65 KB) Additional Information: full citation, references, citings, index terms

10 Application 2: A compact FPGA implementation of the hash function whirlpool
Norbert Pramstaller, Christian Rechberger, Vincent Rijmen
February 2006 **Proceedings of the internation symposium on Field programmable gate arrays FPGA'06**
Publisher: ACM Press
Full text available: pdf(240.32 KB) Additional Information: full citation, abstract, references, index terms

Recent breakthroughs in cryptanalysis of standard hash functions like SHA-1 and MD5 raise the need for alternatives. A credible alternative to for instance SHA-1 or the SHA-2 family of hash functions is Whirlpool. Whirlpool is a hash function that has been evaluated and approved by NESSIE and is standardized by ISO/IEC. To the best of our knowledge only one FPGA implementation of Whirlpool has been published to date. This implementation is designed for high throughput rates requiring a considera ...

Keywords: FPGA, compact hardware implementation, hash function, whirlpool

11 Separating key management from file system security
David Mazières, Michael Kaminsky, M. Frans Kaashoek, Emmett Witchel
December 1999 **ACM SIGOPS Operating Systems Review , Proceedings of the seventeenth ACM symposium on Operating systems principles SOSP '99**, Volume 33 Issue 5
Publisher: ACM Press
Full text available: pdf(1.77 MB) Additional Information: full citation, abstract, references, citings, index terms

No secure network file system has ever grown to span the Internet. Existing systems all lack adequate key management for security at a global scale. Given the diversity of the Internet, any particular mechanism a file system employs to manage keys will fail to support many types of use.We propose separating key management from file system security, letting the world share a single global file system no matter how individuals manage keys. We present SFS, a secure file system that avoids internal ...

12 A low-bandwidth network file system
Athicha Muthitacharoen, Benjie Chen, David Mazières
October 2001 **ACM SIGOPS Operating Systems Review , Proceedings of the eighteenth ACM symposium on Operating systems principles SOSP '01**, Volume 35 Issue 5
Publisher: ACM Press
Full text available: pdf(1.29 MB) Additional Information: full citation, abstract, references, citings, index terms

Users rarely consider running network file systems over slow or wide-area networks, as the performance would be unacceptable and the bandwidth consumption too high. Nonetheless, efficient remote file access would often be desirable over such networks---particularly when high latency makes remote login sessions unresponsive. Rather than run interactive programs such as editors remotely, users could run the programs locally and manipulate remote files through the file system. To do so, however, wo ...

13 A compact and fast hybrid signature scheme for multicast packet authentication
Pankaj Rohatgi
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(759.34 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper proposes a compact and fast hybrid signature scheme that can be used to solve the problem of packet source authentication for multicast. This scheme can be viewed as an improvement to off-line/on-line signature schemes, in that the signature size overhead is much smaller. Since this is a generic technique, it should have applications to several other practical problems as well.

14 Crypto-based identifiers (CBIDs): Concepts and applications
Gabriel Montenegro, Claude Castelluccia
February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1
Publisher: ACM Press
Full text available: pdf(262.76 KB) Additional Information: full citation, abstract, references, index terms, review

This paper addresses the identifier ownership problem. It does so by using characteristics of Statistical Uniqueness and Cryptographic Verifiability (SUCV) of certain entities which this document calls SUCV Identifiers and Addresses, or, alternatively, Crypto-based Identifiers. Their characteristics allow them to severely limit certain classes of denial-of-service attacks and hijacking attacks. SUCV addresses are particularly applicable to solve the address ownership problem that hinders mechani ...

Keywords: Security, address ownership, authorization, group management, mobile IPv6, opportunistic encryption

15 Operating systems security: Attestation-based policy enforcement for remote access
Reiner Sailer, Trent Jaeger, Xiaolan Zhang, Leendert van Doorn
October 2004 **Proceedings of the 11th ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(261.52 KB) Additional Information: full citation, abstract, references, index terms

Intranet access has become an essential function for corporate users. At the same time, corporation's security administrators have little ability to control access to corporate data once it is released to remote clients. At present, no confidentiality or integrity guarantees about the remote access clients are made, so it is possible that an attacker may have compromised a client process and is now downloading or modifying corporate data. Even though we have corporate-wide access control over ...

Keywords: remote access, security management, trusted computing

16 Signature schemes based on the strong RSA assumption
Ronald Cramer, Victor Shoup
August 2000 **ACM Transactions on Information and System Security (TISSEC)**, Volume 3 Issue 3
Publisher: ACM Press
Full text available: pdf(168.52 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We describe and analyze a new digital signature scheme. The new scheme is quite efficient, does not require the signer to maintain any state, and can be proven secure against adaptive chosen message attack under a reasonable intractability assumption, the so-called strong RSA assumption. Moreover, a hash function can be incorporated into the scheme in such a way that it is also secure in the random oracle model under the standard RSA assumption.

Keywords: RSA, digital signatures, provable security

17 An end-to-end approach to host mobility
Alex C. Snoeren, Hari Balakrishnan
August 2000 **Proceedings of the 6th annual international conference on Mobile computing and networking**
Publisher: ACM Press
Full text available: pdf(1.35 MB) Additional Information: full citation, abstract, references, citings, index terms

We present the design and implementation of an end-to-end architecture for Internet host mobility using dynamic updates to the Domain Name System (DNS) to track host location. Existing TCP connections are retained using secure and efficient connection migration, enabling established connections to seamlessly negotiate a change in endpoint IP addresses without the need for a third party. Our architecture is secure—name updates are effected via the secure DNS update protocol, while TCP ...

18 History-based access control for mobile code
Guy Edjlali, Anurag Acharya, Vipin Chaudhary
November 1998 **Proceedings of the 5th ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(1.33 MB) Additional Information: full citation, references, citings, index terms

19 Design and Implementation of the AEGIS Single-Chip Secure Processor Using Physical Random Functions
G. Edward Suh, Charles W. O'Donnell, Ishan Sachdev, Srinivas Devadas
May 2005 **ACM SIGARCH Computer Architecture News , Proceedings of the 32nd Annual International Symposium on Computer Architecture ISCA '05**, Volume 33 Issue 2
Publisher: IEEE Computer Society, ACM Press
Full text available: pdf(288.96 KB) Additional Information: full citation, abstract, index terms

Secure processors enable new applications by ensuring private and authentic program execution even in the face of physical attack. In this paper we present the AEGIS secure processor architecture, and evaluate its RTL implementation on FPGAs. By using Physical Random Functions, we propose a new way of reliably protecting and sharing secrets that is more secure than existing solutions based on non-volatile memory. Our architecture gives applications the flexibility of trusting and protecting only ...

20 Chord: A scalable peer-to-peer lookup service for internet applications
Ion Stoica, Robert Morris, David Karger, M. Frans Kaashoek, Hari Balakrishnan
August 2001 **ACM SIGCOMM Computer Communication Review , Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM '01**, Volume 31 Issue 4
Publisher: ACM Press
Full text available: pdf(205.73 KB) Additional Information: full citation, abstract, references, citings, index terms

A fundamental problem that confronts peer-to-peer applications is to efficiently locate the node that stores a particular data item. This paper presents *Chord*, a distributed lookup protocol that addresses this problem. Chord provides support for just one operation: given a key, it maps the key onto a node. Data location can be easily implemented on top of Chord by associating a key with each data item, and storing the key/data item pair at the node to which the key maps. Chord adapts effi ...

Results 1 - 20 of 191 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Sign in

Web Images Groups News Froogle Local **more »**

sha-1 and csa and cla Search Advanced Search Preferences

The **"AND"** operator is unnecessary – we include all search terms by default. [details]

Web Results **1** - **10** of about **799** for **sha-1 and** **csa and cla**. (**0.37** seconds)

EP1360795
... the fixed-size data blocks using an **SHA-1** multi-round ... hash round logic for an **SHA1** authentication algorithm ... one 5-bit addition, one 32-bit **CSA**, a multiplexer ...
swpat.ffii.org/pikta/txt/ep/1360/795/ - 49k - Supplemental Result - Cached - Similar pages

[PDF] AN EFFICIENT IMPLEMENTATION OF HASH FUNCTION PROCESSOR FOR IPSEC
File Format: PDF/Adobe Acrobat - View as HTML
applications of **SHA-1**, MD5, HAS-160 and other hash functions. to generate MACs. ... 8-bit **CLA** (carry look-ahead adder), **CSA** (carry select adder) and ...
www.ap-asic.org/2002/2B-4.pdf - Similar pages

Cisco Security Advisory: Crafted Timed Attack Evades Cisco ...
... BEGIN PGP SIGNED MESSAGE----- Hash: **SHA1** Cisco Security ... com/warp/public/707/cisco- sa-20041111-**csa**.shtml ... Format string vulnerability; Next by Date: [**CLA**-2004:889 ...
cert.uni-stuttgart.de/archive/ bugtraq/2004/11/msg00153.html - 15k - Supplemental Result - Cached - Similar pages

[PDF] Divide-and-Concatenate: An Architecture Level Optimization ...
File Format: PDF/Adobe Acrobat - View as HTML
... not sufficient [5]. Furthermore, implementing MD5 and **SHA-1** in hardware ... Commercial implementations of MD5 and **SHA1** targeting 0.18 ... gates rpl **cla** bk **csa** 1-stage 2 ...
www.dac.com/.../0c4c09c6ffa905c487256b7b007afb72/ a25aec1c2384a70d87256e54007a1dfe/$FILE/35_4.PDF - Supplemental Result - Similar pages

United States Patent Application: 0020001384
an Authentication engine architecture for an **SHA1** Authentication algorithm, ... c and d by an add5to1 adder module that is built by **CSA and CLA** adders. ...
appft1.uspto.gov/.../ 20020001384&RS=DN/20020001384 - 55k - Supplemental Result - Cached - Similar pages

[PDF] Security Gateway 3100 Series
File Format: PDF/Adobe Acrobat - View as HTML
Safety: UL, CUL, **CSA**, CB. EMC: FCC class A, BSMI, CE class A, C-Tick, VCCI class A. Enviromental ... **CLA**-APP-SG3110-SG3150. Clavister Security Gateway 3150 ...
www.abox.com/PDFM/Clavister_ Security_Gateway_3100_Series_Brochure.pdf - Similar pages

[PDF] Security Gateway 4400 Series
File Format: PDF/Adobe Acrobat - View as HTML
Safety: UL, CUL, **CSA**, CB. EMC: FCC class a, BSMI, CE class a, C-Tick, VCCI class a ... **CLA**-APP-SG4410-DC. Clavister SG4410. Failover Unit AC power supply ...
www.genusai.com/Docs/sg4400.pdf - Supplemental Result - Similar pages

[PDF] _PAPER PREPARATION KIT FOR THE
File Format: PDF/Adobe Acrobat - View as HTML
... **SHA-1** algorithm consists of four rounds of processing of 20 ... delay, we implemented high speed adder using **CLA** (carry look-ahead adder) and **CSA** (carry save ...